A STRATEGIC ANALYSIS OF STATIONARY RADIATION PORTAL MONITORS AND MOBILE DETECTION SYSTEMS IN BORDER MONITORING

A Thesis

by

RYAN CHRISTOPHER COOGAN

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Chair of Committee,	Craig Marianno
Committee Members,	Sunil Chirayath
	Arnold Vedlitz
Head of Department,	John Hurtado

May 2019

Major Subject: Nuclear Engineering

ABSTRACT

Radiation Portal Monitors (RPM) are our primary border defense against nuclear smuggling, but are they still the best way to spend limited funds? The purpose of this research is to strategically compare RPM defense at the border with state-side mobile detectors. The challenge of an adequately detailed smuggling network problem is that the number of variables required to adequately capture the problem also makes the problem computationally exhaustive. A well bounded problem, although simple, can provide meaningful information to a decision-maker. Limiting the problem to a comparison of two technologies, a decision-maker can prioritize how to best allocate resources, by reinforcing the border with stationary Radiation Portal Monitors (RPMs) which can be perceived, or by investing in Mobile Radiation Detection Systems (MRDS) which are harder for an adversary to detect but may have other weaknesses. An abstract, symmetric network is studied to understand the impact of initial conditions on the network, and the most conservative choices are made in an asymmetric network loosely modeled on the state of Texas transportation system. This asymmetric network is then examined for the technology that will maximally suppress the adversary's success rate at minimal cost. We conclude that MRDS, which have the advantage of discrete operation, outperform RPMs deployed to a border. We also conclude that MRDS maintain this strategic advantage if they operate with one-tenth the relative efficiency of their stationary counter-parts or better.

DEDICATION

This thesis is dedicated to my wife, Sara Catherine Hart, who has been my rock in the choppiest of waters and continues to inspire, and to my great friend Zachary Edwin William Parsons, whose faith in me has never wavered. It is my sincerest hope that I can live up to the example both have set before me.

ACKNOWLEDGEMENTS

I would like to thank my committee chair, Dr. Craig Marianno, who was instrumental in seeing this work ushered to completion and who has truly been both a great critic and a great supporter of my work over the years.

Special thanks also to my initial mentor, Dr. William Charlton, who took a chance on an unlikely candidate to the field, posed the question, and provided great insight into modeling.

I would also to thank my committee members, Dr. Arnold Vedlitz and Dr. Sunil Chirayath for their time, patience, and dedication.

Thanks also go to my friends and colleagues in the department for making my time at Texas A&M University a great experience.

I also want to extend my gratitude to the staff, in particular Robb Jenson, whose contributions are often unsung but also indispensable.

Finally, thanks to my friends and family both inside and outside of Aggieland, who provided strength and encouragement.

CONTRIBUTORS AND FUNDING SOURCES

Contributors

This work was supervised by a thesis committee consisting of Professor Craig Marianno, advisor, and Professor Sunil Chirayath of the Department of Nuclear Engineering and Professor Arnold Vedlitz of the Department Political Science.

Assistance in modeling techniques was provided by Professor William Charlton of University of Texas.

All other work conducted for the thesis was completed by the student independently.

Funding Sources

Graduate study was supported by a fellowship from Texas A&M University and the Center for Nuclear Security Science and Policy Initiatives (NSSPI).

TABLE OF CONTENTS

LIST OF FIGURES

Page

LIST OF TABLES

Page

1. INTRODUCTION AND BACKGROUND

"The danger of nuclear terrorism is the greatest threat to global security [1]"

This thesis examines the payoffs of continued investment into the infrastructure of Radiation Portal Monitors (RPMs) contrasted by diversifying into Mobile Radiation Detection (MRDs). Analysis of a transportation network, which already has a RPM component, will demonstrate that investment in mobile radiation detection, rather than additional RPMs, is a superior defense against non-state actors.

Nuclear terrorism and the threat thereof is a new phenomenon, even considering the youth of nuclear technology in general. Traditionally, terrorists do not inflict massive harm on civilians, instead choosing enough violence to shock the public without completely repulsing potential supporters. Traditional terrorism is a form of drama, or psychological warfare whose victims are the viewing audience rather than the casualties [2]. Traditional terrorist groups have finite goals and objectives that demand selective targeting and calibrated force. The goal of this drama is not to inflict maximum casualties but to win public support and erode confidence in the state [3]. The massive casualties of a nuclear weapon do not interest traditional groups, and even the threat of one for purposes of blackmail or ransom are too costly and uncertain [2].

Conversely, non-traditional groups may not have finite or even realistic objectives. These groups may not need public support. Indeed, they often do not even want it. Such terrorists are primarily interested in lashing out against society for

perceived wrongs and inflicting the maximum amount of pain and suffering on their enemy [4]. For these groups nuclear terrorism may be an option.

1.A. Characteristics of the Nuclear Terrorist

The aspiring nuclear terrorist is very likely a non-traditional actor. The actor of interest is a small cell or a large, organized group. Lone actors may have an interest in nuclear terrorism, however, because of their limited capabilities and resources their probability of conducting a successful attack is diminishingly small. There are three generally accepted pathways by which a non-state adversary might acquire a nuclear weapon – state transfer of a weapon, material, or components; theft; or manufacture – none of which can be accomplished by a lone actor. History supports this. For example, a study of 45 radiological and nuclear terrorist plots by Ackerman et. al. demonstrates that nuclear terrorism is the purview of small cells and large, organized groups [5].

The probability of state sponsorship is generally considered to be extremely low [6]. The state sponsor would have to be either reckless, desperate, or unusually confident in the terrorist organization because the cost of having a weapon attributed through intelligence or forensics is nuclear retaliation [7]. The threat of retaliation serves as a significant deterrent for potential sponsors – even those who typically sponsor terrorism or traffic in conventional weapons [8].

Weapons are generally well protected because the state depends on secure weapons to maintain deterrence capabilities. Sophisticated weapons contain advanced security features such as a permissive action links (PAL) – a built-in security measure

that prevents unauthorized detonation. However, even less sophisticated weaponry is generally kept in secret facilities and well protected, sometimes with financial and technical assistance from other powers with a vested interest in nuclear security (such as the United States assistance providing PAL assistance to Pakistan under the Bush administration) [9].

The most probable pathway for a terrorist to acquire and use a nuclear weapon is to manufacture an improvised nuclear device (IND) using fissile material and a crude triggering device to initiate a chain reaction. An IND would be significantly less powerful than a state device, but could still produce a yield equivalent to some kilotons of dynamite. Therefore, the theft and trafficking of nuclear material is a significant concern and is specifically addressed as the greatest threat to global security in America's counter terrorism strategy [1].

Acquiring fissile material is considered by many experts to be the most difficult step for the aspiring nuclear terrorist. However, the IAEA's Illicit Trafficking Database contains 16 incidents of trafficking in uranium or plutonium between 1993 and 2011 [10]. Because the IAEA is not an investigative body and only reports numbers that states are willing to confirm, the actual number of trafficking incidents may be higher. While none of these incidents alone poses a threat, it does demonstrate nuclear trafficking is real and with it the possibility (likely or not) of nuclear terrorism. Although the probability of a nuclear event is highly unlikely, the high consequences associated with it means that the United States has good reason to invest in infrastructure

to detect and deter non-state adversaries who may choose to execute a nuclear option on American soil.

1.B. Security Infrastructure

American nuclear security is a multi-stage process that begins with enhancing security of foreign nuclear material, and therefore denying nuclear material at the source. That security extends to detection, interdiction, and response at the borders of foreign nations and continues to America's borders where RPMs can detect nuclear materials moving through the border.

RPMs are passive systems that can detect nuclear and radiological materials in vehicles, containers, and on persons passing through them. There are a number of different configurations for portal monitors; however, the most common configuration is double-sided where two detectors are placed on opposite sides of a controlled lane to scan objects of interest [11] (Figure 1). Single-sided systems are less common because they are less effective. Even less common are multi-sided systems where the object of interest is enclosed on three or more sides for scanning.

First generation RPMs were composed of helium-3 tubes used for neutron detection of special nuclear materials (SNM) and polyvinyl toluene (PVT) plastic slabs to detect gamma radiation. These RPMs still compose the bulk of RPMs deployed to the U.S. border [11]. However, the helium-3 shortage has forced manufacturers to find alternative solutions, such as boron-10 lined ZnS(Ag) scintillators developed for neutron and gamma detection capability [12].

Figure 1. Radiation Portal Monitor (RPM) in an exit lane. This RPM uses a standard double-sided configuration. Reprinted from "United States Customs and Border Protection's Radiation Portal Monitors at Seaports." **Error! Bookmark not defined.**

Secondary components process and calibrate the electronic signals from the detectors to discriminate passive background radiation, minimize false alarms, and communicate true positives to security personnel. The geometric configuration, physical components, and software settings means there is some variance in detector capability from one to the next. However, ANSI standards set a maximum false alarm rate (less than 1 in 1000 occupancies) and a minimum true positive rate (at least 59 of 60 occupancies) [13]. Manufacturers are often capable of exceeding these standards [13], but may advertise minimum detectable quantities in an ideal environment where very few detectors have the luxury of operating.

Vehicles and persons that produce an alarm are sent for secondary screening. If secondary screening verifies a signal, U.S. Customs and Border Protection (CBP) officers use hand-held detectors to isolate, locate, and identify the source. The complete process for clearing an alarm is shown in Figure 2.

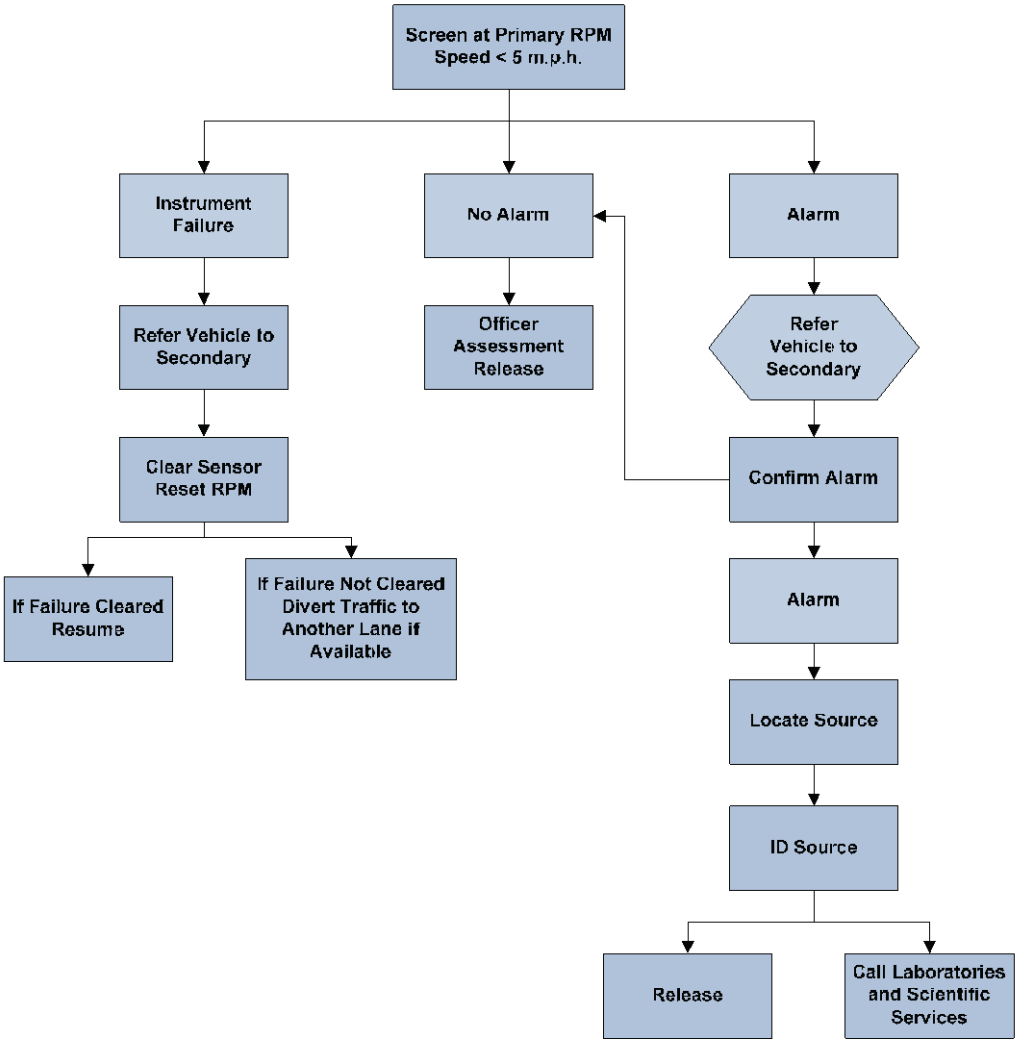

Figure 2. Customs and Border Protection (CBP) process for resolving alarms. Reprinted from "United States Customs and Border Protection's Radiation Portal Monitors at Seaports" [11].

Improvements in technology and the commercialization of radiation detectors have made mobile radiation detection systems (MRDs) another option that can support security. Mobile systems are housed in trucks, vans, or SUVs that can be deployed to

major thoroughfares or surged to protect a potential target, interdicting actors that have breached the border.

1.C. Nuclear Smuggling Network Modeling

A number of network interdiction models have been developed and studied over the last decade. In his seminal work, Wood developed a deterministic model for analyzing commodity smuggling wherein an interdictor with limited resources seeks to minimize an adversary's commodity trafficking across a capacitated network [14]. Wood demonstrated that even this basic problem, solving for the interdictor's cost-effective investment, is computationally exhaustive. Although this model was designed for commodity smuggling, such as drugs or weapons, Wood's observation is still informative in analyzing nuclear smuggling and necessitates a practical and measured examination of any network. Wood coped with these limitations by developing a new integer programming model, however, this model needs bulwarking if the network is sufficiently complex. Additionally, while this does significantly decrease computational time, a given network may still be too computationally exhaustive to study.

Recent studies have had success in studying networks that were sufficiently well-defined or limited in scope as a way of coping with uncertainty. Dimitrov et al. constructed a stochastic network where an interdictor installs detectors on a network that are transparent to a nuclear-smuggler [15]. The smuggler seeks to evade detection while the interdictor seeks to minimize the smuggler's probability of success. Dimitrov copes with the computational challenge that Wood discovered by inverting the data stream,

turning the unknown resources that Wood tried to calculate into a known input instead. Under a known threat scenario, with known detection probabilities, this stochastic model plots the most effective deployment of detectors.

Cheng et. al. demonstrated the viability of a mobile sensor network where simple radiation detectors are mounted in vehicles [16]. Cheng limits the scope of the problem with a mobile system that is extremely dense, approximately 3,000 units to cover the island of Manhattan; using non-detection probabilities that fall within a specified range and which preclude challenges associated with varying shielding; and with perfect knowledge of where every sensor is located at any given time. The model is not comprehensive but does provide a clear indication whether such a system is advantageous to pursue as a practical exercise.

While some effort has been invested in strategies to quantify the uncertainties surrounding an adversary[17], very little attention has been paid to the uncertainties associated with the interdictor. Simply put, too many models assume the interdictor has perfect knowledge of the network. Israeli and Wood acknowledge that adversaries may have access to pathways that are immune to the influence of an interdictor [18]. The number of cross-border tunnels that have been discovered in recent years to smuggle narcotics into the United States – more than 140 of them between 1990 and 2012 – is evidence enough that Israeli and Wood were correct [19]. A practical model must consider that there may be nodes and pathways that the interdictor cannot influence or may not even know exist. At the very least, the problem must be constrained such that the interdictor can never have perfect certainty of the smuggler's network.

Haphuriwat et al conclude that in the absence of perfect knowledge and perfect detection capability, the only successful strategy is one that compensates for imperfect detection capability (and knowledge) with a sufficiently credible threat of retaliation [20]. Certainly the United States has invested in advertising its capabilities and its policy of retaliation toward a nuclear strike. However, it can also benefit from at least understanding the uncertainties associated with the problem of nuclear smuggling and thereby improve its ability to detect and deter potential adversaries.

A comprehensive model may be intractable, however, a model that examines a particular scenario can be sufficiently limited to provide a solution that is informative for decision makers; for example, the placement of detectors along the U.S. border given a fixed budget and detectors of a known capability [15]. Assumptions and simplifications make models less realistic but are necessary to make models computationally tractable and informative. Alternatively, these models can be solved by breaking down a single network problem into a series of independent submodels [21]. Even this effort requires some measure of assumption and simplification to aggregate information from the submodels into a coherent strategy.

The research presented in this work makes several assumptions and simplifications, justified by the narrow scope of the research objective, and by the computational limits of comprehensive network modeling. These assumptions include a network model where the adversary has access to routes which are immune to the interdictor's influence, where the interdictor's detection capabilities are known with

certainty, but the adversary's success is uncertain and expressed as a probability. These assumptions and the scope of this research are detailed below.

1.D. Research Objective

This thesis is concerned with inferring decisions associated with the following question: Given an existing infrastructure with imperfect coverage of the border, and given an adversary of sufficient technological and conventional capabilities to attempt a nuclear smuggling operation, are decision-makers best served with continued investment into stationary RPMs deployed along the border or investment into mobile units operating within U.S. borders?

We limit the problems typically associated with network modeling by framing the problem as one of relative utilities. Will RPMs effect adversary failure more than MRDs? What is the break-even point where neither option is preferred? Quantifying the true impact of one system or another on an actual network is not the scope of this project. Instead this thesis is concerned only in answering which option outperforms the other on a strategic level.

Neither does this project attempt to solve the challenge of uncertainty for the interdictor, although it does acknowledge that any model that depends on perfect knowledge is theoretical and deeply flawed for practical purposes. This project addresses interdictor uncertainty by modeling the adversary's transportation network, which may overlap with the interdictor's network in many areas but not all.

2. THE SHIELD NETWORK INTERDICTION MODEL

The strategic problem of analyzing a transportation network can be examined with a modeled network composed of nodes and pathways[15]. Nodes represent specific physical locations such as airports, border crossings, seaports, etc. Whereas pathways represent a transportation path available to an adversary vis-à-vis roadways, rail, boat, etc. that connects two nodes. Nodes are the end-points and midpoints for all pathways, representing entry points into the network, the target destination, and midpoint opportunities (such as junctions or a change in transport). A simple network is illustrated in Figure 3. Nodes are denoted by circles and pathways are denoted by arrows showing the direction of flow across the network. Node 1 is the origin and Node 3 is the target or destination, while Nodes 2 and 4 are intermediary nodes that may represent a change from one roadway to another, or even from one vehicle to another such as with a port.

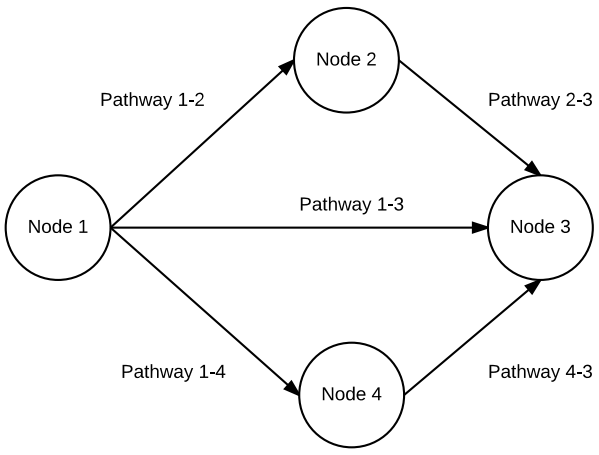

Figure 3. A simple network with four nodes and three pathways.

SHIELD is a code developed by Jun Luo at the Nuclear Security Science and Policy Institute (NSSPI) to analyze the strategic problem of nuclear smuggling. An input deck provided by the user generates a network with a starting node, a target node, and a network of intermediary nodes and pathways. The user specifies the non-detection probabilities associated with each node and pathway where the non-detection probability is the probability that an adversary will not be detected when traversing an element of the network. Each node and pathway has an associated perceived non-detection probability (*Per nPD*), which is used to calculate the adversary's preferences in routes; conversely the actual non-detection probability (*Act nPD*) is used in calculating the adversary's expected success in traversing the network.

The network can be constructed with varying parameters for different types of adversaries. A sophisticated adversary will assess the entire network and prioritize routes that have the highest overall chance for success; whereas an opportunist will proceed step-by-step across the network, selecting pathways based on the path of least resistance immediately available. Other adversary types, such as insiders, are not modeled in SHIELD; however, it may be possible to account for them either in the network itself or by perturbing the non-detection probabilities of select nodes and pathways. Failure is measured simply by the adversary's interdiction before reaching the target node.

SHIELD linearizes all routes across the network, eliminating low probability and zero-success routes in favor of high success routes until the code has the user-defined maximum number of routes. A Monte Carlo method is used to determine the adversary's

successes and failures across multiple routes. SHIELD then aggregates the successes and failures of the adversary across all routes of interest to calculate the adversary's overall success, expressed as a percentage of attempts.

A sample input deck can demonstrate the set-up and limitations of SHIELD. A full input deck for a sample network can be found in Appendix A, while Figures 4 and 5 below are excerpts from the sample network. Figure 4 illustrates setup information for the SHIELD input deck. Run number is the number of runs that SHIELD will execute. HEU quality is the enrichment of material, and container type quantifies the level of shielding in the surrounding container - these are not working features of SHIELD yet, however source and shielding can be accounted for simply by setting the actual non-detection probability to the expected value. The print controls simply determine what information is printed in the output file. The second command line contains behavior, routes, and seed inputs. Behavior determines if the adversary is intelligent (0) or opportunist (1) which governs the manner in which they traverse the network (as above). The routes number is the maximum number of routes that SHIELD will linearize for sampling. The random number generation starts from a seed value. If the same seed is selected, then SHIELD will produce the same results on the same model. Seed method can be set to either a 0 or 1, which will determine if SHIELD uses a seed value from the clock to generate random values, or if it uses a fixed seed value. Layers are used for back-calculating a maximum success rate for the adversary. After completing a run, SHIELD can perturb layers of the network within the range of values assigned to

optimize the network for a given success rate. The final command line simply tells SHIELD the number of nodes in the network and which node is the target node.

```
C----------------------------------------
C
C   SHIELD program version 1.33.0.0
C   Developed By Nuclear Security Science & Policy Institute (NSSPI)
C   Saved Input file
C   Saved Date and Time: 7/30/2015 2:18:16 PM
C
C----------------------------------------
C
C   run_number, HEU_quality, Container_type
       100000;        20.5;              3;
C
C (print control) Title, Summary, Input, Bin, Routes, Links, Nodes
                     1;       1;     1;   1;      1;     1;     1;
C
C Behavior mode, routes num, seed method, seed value
             0;          10;           1;         10;
C
C Total dataset number
10;
C Layer Num, Min nPD lim, Max nPD lim;
1;                   0.1;         0.9;
2;                   0.1;         0.9;
3;                   0.1;         0.9;
4;                   0.1;         0.9;
5;                   0.1;         0.9;
6;                   0.1;         0.9;
7;                   0.1;         0.9;
8;                   0.1;         0.9;
9;                   0.1;         0.9;
10;                  0.1;         0.9;
C
C Node number, initial node, end node
           26;           99;       26;
```

Figure 4. Excerpt of a sample input deck header for SHIELD. This excerpt includes setup information for the network.

Figure 5 contains an excerpt from the body of the sample input deck. The first command line includes all relevant information for a node, starting with the "N" designation for node and an assigned number. The perceived non-detection probability (Per nPD) determines the adversary's behavior whereas the actual non-detection probability (Act nPD) determines the adversary's success or failure. For a sophisticated adversary these values may be the same (as demonstrated below). Forward paths tells SHIELD how many paths to anticipate flowing forward from the node, time is the number of hours the adversary is held at the node, and redirect probability is the random

probability that the adversary will be redirected to an alternate route rather than staying on course. Origin and locations are strictly for the user's convenience. Latitude and longitude are used in plotting the network on SHIELD's graphic interface; these can be used to calculate the real distance along paths or ignored and used exclusively for the user's convenience.

Below the node command line are all pathways moving forward from that particular node. Pathways are denoted by the "P" command, in the first column, with an initial and ending node. Distance can be set by the user in miles, or as described above can be calculated using the shortest geodesic for a globe. Time is the number of hours that the adversary is on the path. Pathways have a perceived and actual non-detection capability just as nodes do.

```
C - 1, node no., Per nPD, Act nPD, forward paths, time, redirect_prob,layer,    description, location,    lat,       long,
N;          99;     0.6;     0.6;             3;    2;          0.3;    1;    Origin;       Ozersk;     55.7500;   60.7167;
C - Pathway from node   1, initial node, end node, layer, distance, time, Per nPD, Act nPD, description
P;                                 99;        2;     2;   100.00;    2;     0.7;     0.8;        NONE;
P;                                 99;        4;     2;   200.00;    3;     0.7;     0.7;        NONE;
P;                                 99;        9;     2;   400.00;  2.5;     0.8;     0.9;        NONE;
C
C - 2, node no., Per nPD, Act nPD, forward paths, time, redirect_prob,layer,    description, location,    lat,       long,
N;           2;     0.8;     0.9;             1;    3;          0.2;    1; Reload on truck;  unknown;   55.7153;   60.5442;
C - Pathway from node   2, initial node, end node, layer, distance, time, perceived nPD, actual nPD, description
P;                                   2;        5;     2;   200.00;    4;           0.7;        0.7;        NONE;
C
C - 3, node no., Per nPD, Act nPD, forward paths, time, redirect_prob,layer,    description, location,    lat,       long,
N;          3;       0.8;    0.75;             1;    4;          0.4;    3;     port;  Vladivostok, RU;  43.1058;    131.9162;
C - Pathway from node   3, initial node, end node, layer, distance, time, perceived nPD, actual nPD, description
P;                                   3;       19;     3;    30.00;    1;           0.6;        0.8;        NONE;
```

Figure 5. Excerpt of a sample input deck body for SHIELD. This excerpt includes information on the network's nodes and pathways.

It is worth noting several features of SHIELD's operation. Time is summed for all nodes and pathways on a single route. This data is then aggregated for all attempts, yielding an average time for the adversary's interdiction (in the case of failure) or an average time for the adversary to completely traverse the network (in the case of

success). This has no direct impact on the adversary's success or failure and may best be utilized in problems studying delay strategies for a surge response.

3. ASSUMPTIONS ABOUT THE NETWORK

The goal of this work is an informative, comparative analysis of two networks. This work is not intended to be fully comprehensive, but instead to inform a single choice. In order to address the question meaningfully, assumptions have been made to create a solvable network model.

RPMs are modeled as nodes in a border region with a static detection probability greater than zero. It is assumed that all RPMs have the same detection probability. This is not actually true. Variations exist between detector types, software, geometry, and the procedure for implementation. These are not trivial differences in the lab, but are considered insignificant for the strategic problem of determining adversary preferences. For all RPMs the detection probability is assumed to be 0.98 based on ANSI standards[22], and therefore the non-detection probability is 0.02.

MRDS are modeled as pathways with a detection probability greater than zero. The detection capability of MRDs is assumed to be equivalent to that of RPMs, because ANSI standards for both systems are exactly identical for the purposes of evaluating a system non-detection probability [22], [23]. However, MRDs have significantly less control over geometry and implementation than RPMs because of the manner in which they are used, which may include discrete operations. Therefore, this thesis also considers a range of possible values for MRD efficiencies relative to RPMs, such that:

$$P_{MRD} = P_{RPM} * \varepsilon$$

where P_{MRD} is the detection probability of the MRD unit, P_{RPM} is the detection probability of the RPM unit, and ε is the fractional difference in efficiency between an RPM which operates in practically ideal circumstances, and the MRD which does not.

MRDs are modeled as a detection capability on pathways of the network. MRDs are centered on a node inside the border and traverse adjacent pathways feeding in or out of this node. It is assumed that the MRD has no downtime and that there is an equal probability that the MRD unit will be deployed to any of its adjacent pathways. The probability (p) that a MRD unit is on any given pathway at any given time is $p = \frac{1}{n}$ where n is the number of adjacent pathways. Therefore, the non-detection probability for a pathway is:

$$\beta_{i,j} = 1 - \frac{P_{MRD}}{n_i}$$

where $\beta_{i,j}$ is the non-detection probability of a pathway connected to deployment node i and node j, n_i is the number of paths connected to deployment node i, and P_{MRD} is the detection probability of the MRD unit.

An illustration of MRD modeling is provided in Figure 6 below. Node 2 is the deployment node (i). The adversary can only move forward toward the target (denoted by arrows), but the mobile unit can be positioned on any adjacent pathway. All pathways moving in or out of the deployment node are potential routes (n) for the MRD

and will have a non-detection probability determined by the formula given above. For an ideal system where the MRD has perfect detection capabilities $\beta_{1,2} = 0.333$.

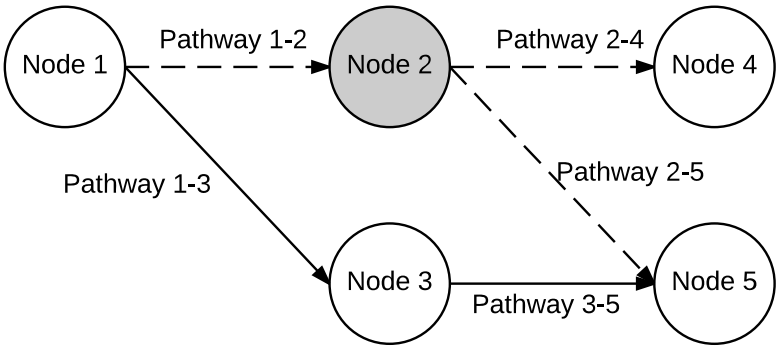

Figure 6. Sample deployment node and pathways. Node 2 is the deployment node for an MRD unit. Pathways 1-2; 2-4; and 2-5 will have an increased detection capability as a result.

This thesis is a comparative assessment of two technologies, and therefore our primary focus is how these technologies impact the strategic problem of nuclear smuggling. RPMs and MRDs operating in the field do not have the idealistic non-detection probabilities assumed here. Because this research is a comparative assessment of two technologies it is not necessary to perfectly characterize these probabilities. Instead, we only need to characterize them relative to each other, and the baseline ANSI standard does that.

Additionally, because this is technological assessment, it is assumed that RPMs and MRDs dominate the non-detection probabilities associated with the network. In truth, the non-detection capability of a real network at any given point is a confluence of technology, law enforcement, and other factors. Quantifying the indigenous non-

detection probability of law enforcement is challenging because it depends on a number of factors that vary based on the behavior of the adversary or state agencies. Routine traffic stops can be used to derive an expected value for the effectiveness of indigenous law enforcement when there is no actionable intelligence or information about the adversary.

In 2011 the Department of Justice reported approximately 10.2% of the nation's 212.3 million drivers were targeted by a traffic stop [24]. That averages to 0.028% of all drivers per day, assuming of course that all drivers operate a vehicle daily. This assumption is not realistic and the probability of a traffic stop occurring in a single day for the adversary is virtually zero. A more realistic approach would examine the length of the smuggler's trip because the longer the smuggler is in the open the greater the risk.

The Department of Transportation reports that the average driver is on the road 13,476 miles annually [25]. If only 10.2% of 212.3 million drivers are subject to a traffic stop, the average driver will cover 132,118 miles before being stopped, which is roughly equivalent to driving the breadth of the continental United States 37 times. It can be argued that the average driver is not a nuclear smuggler, and the smuggler may share risk-tolerant characteristics consistent with drivers who are stopped more frequently. Adults aged 20-34 drive 15,098 miles per year [25]**Error! Bookmark not defined.**, make up 12.7% of all drivers but account for 22.5% of all traffic stops[24]. The expected number of miles between traffic stops for a driver between the ages of 20 and 34 is 83,992 miles, which is still far too high to be useful in a model where the adversary is unlikely to travel even 1,000 miles because high-value targets (namely cities) tend to

be close to physical borders, or ports, or both. Unless any given route varies considerably in length, by three or more orders of magnitude, the indigenous detection probability will be overwhelmed by random error associated with the sampling technique.

Therefore, indigenous detection probabilities are not considered in this model. The non-detection capabilities for this network were calculated exclusively from the capabilities of RPMs and MRDs. Nodes and pathways that were not supported by RPMs or MRDs were assigned a non-detection probability of unity.

4. ASSUMPTIONS ABOUT THE ADVERSARY

This thesis considers the most conservative case – an intelligent adversary that is technically sophisticated, capable, and well-funded. It is assumed that such an adversary can effectively assess the border for RPMs and minimize exposure by exploiting smuggling routes and illegal entry points to cross the border – see Figure 7 for an example of the overt nature of RPMs. Such an adversary is unlikely to be a lone-wolf or an opportunist, whom RPMs are well situated to detect. Instead this thesis considers the capabilities posed by an organized group with significant conventional and nuclear capabilities.

Figure 7. U.S border crossing with RPMs. RPMs are clearly visible in blue. The overt nature of an RPM at a border crossing means it is trivial for an adversary educated on nuclear materials to identify one and simply avoid it.

Intelligence and conventional capabilities are modeled in the adversary's ability to perceive and rank-order routes across the whole network rather than traversing the network step-by-step. Technical sophistication is modeled as the ability to accurately identify RPMs and assess their non-detection capabilities. Therefore,

$$\beta_j{}^{Per} = \beta_j{}^{Act}$$

where β_j^{Per} is the adversary's perceived non-detection probability for node j and β_j^{Act} is the actual non-detection probability of node j.

It is also assumed that an intelligent adversary may be informed to the presence of MRDs on the network, but is not capable of identifying placement. MRDs can be housed in low-profile automobiles that would make identification very difficult. Further, MRDs may be deployed to a number of potential sites and thoroughfares that can be challenging to scout and plan around. A rational actor may assume there is an equal probability that an MRD is deployed to any given route. This may influence the decision to go nuclear, but it does not help the smuggler avoid detection because all routes are equally attractive and equally not. For pathways that do in fact house MRD capability, the perceived non-detection probability ($\beta_{i,j}{}^{Per}$) will always be less than the actual non-detection probability ($\beta_{i,j}{}^{Act}$). Therefore,

$$\beta_{i,j}{}^{Per} < \beta_{i,j}{}^{Act}$$

5. NETWORK SETUP

A strategic analysis was conducted on two networks – a simple symmetrical network and a more complicated asymmetrical network. Each network was composed of four different regions – pre-border, border, principality, and target (see Figure 8).

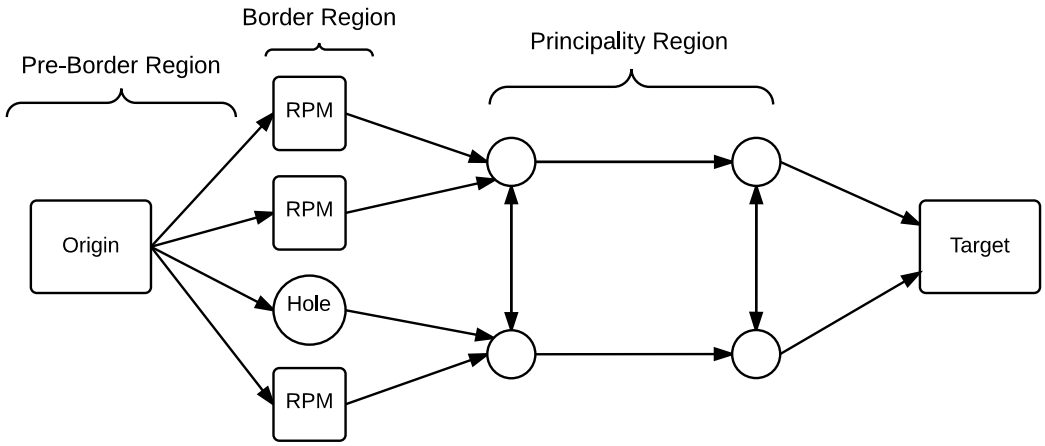

Figure 8. A sample network with four regions.

The pre-border region represents materials outside the border and is used strictly to position material for movement across the border region. The United States has invested heavily in the Second Line of Defense that places RPMs and other capabilities in foreign states with the hope of limiting nuclear trafficking. For the purposes of this analysis the pre-border region had no detection capabilities to ensure that simulations tested only one variable.

The border region represents entry points into the state and is composed of legal border crossings with simulated RPMs and illegal "holes" which have zero-detection capability. The default network has 80% coverage across the border, and legal entry

points are nodes with a perceived and actual non-detection capability of two percent[Error! Bookmark not defined.]:

$$\beta_j^{Per} = \beta_j^{Act} = 0.02$$

The principality region represents pathways and opportunities available inside the border en-route to the target. The default non-detection capability for all pathways and nodes in the principality region is unity. The target region is composed of a single node that the adversary must reach. The target node does not change. Additionally, the target node does not possess any detection capability because the model does not allow the adversary to deviate or pursue any course that does not eventually bring them to the target node. Any detection capability on this node is not actually a deterrent and therefore not considered in this model.

6. SYMMETRIC NETWORK

A symmetric network was analyzed to better inform the creation of an asymmetric network. An asymmetric network better represents the reality of a transportation network, where variance creates chokepoints, break-out opportunities, and other complications. However, the model may be highly sensitive to not just the mapping, but also the distribution of legal and illegal entry points. To explore the impact of that distribution, a symmetric model was created.

The symmetric network was coded into three variations to analyze the system's sensitivity to the initial distribution of holes in the border region – this analysis would then inform the creation of the asymmetric network. The initial construction of the network, without holes, is shown in Figure 9. This new network is composed of 40 border nodes (30 legal entry points and 10 illegal holes), 10 principality nodes, a single origin node, and a single target node. The holes in the border region were distributed randomly, uniformly, and in large clusters to measure the network's sensitivity to these initial conditions. These three networks are called Random, Uniform, and Clustered respectively. The Random distribution was created using a random number generator for node assignments in the border region. The Uniform distribution has holes distributed evenly alongside legal entry points. The Clustered distribution has half of the network's holes at the top of the border region (but not on the edge) and the other half at the bottom of the border region (but not on the edge).

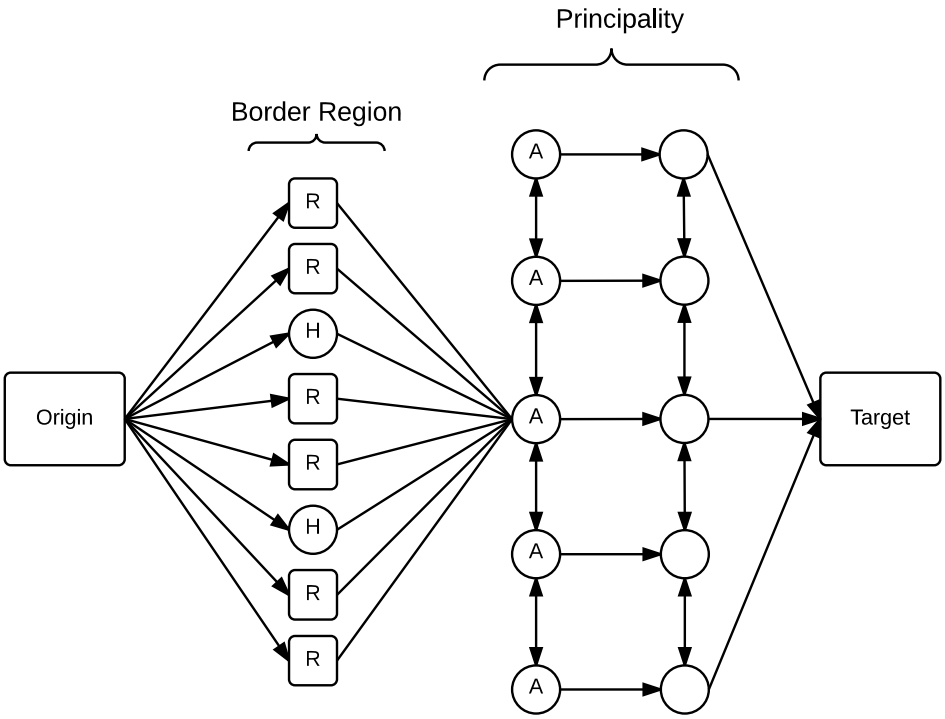

Figure 9. Symmetric network. RPMs are denoted by R and Holes are denoted by H. The Border Region is duplicated five times, connecting to each "A" node in the Principality region. The border in its entirety is composed of 40 nodes. For pictorial sakes, only 8 of the 40 border nodes are shown.

These initial network variants were then subjected to a battery of tests to determine if variables such as distance, time, or redirect probability would affect the adversary's success rate. The results of this sensitivity analysis concluded that perturbing these values did not change the outcome of the model, which was expected. The sensitivity analysis did determine that the network was sensitive to the network's geometry, but this was also anticipated.

6.A. Radiation Portal Monitors

The network was first tested for the sensitivity of RPMs on the initial distribution of holes. Holes in the border region were filled piece-wise at random and tested, until all holes in the border region were closed by RPMs. An initial test using standard non-detection probabilities[Error! Bookmark not defined.] had nearly identical results for all three variants (Table 1). Results varied by at most 0.20 of a percent, which is attributed to random error in Monte Carlo sampling. In Table 1 (below), supplemental RPMs have a negligible effect on adversary success rate until there is one hole in the border region. With one hole in the border region, adversary success drops to 92.7 percent. A pathways analysis revealed that this was because SHIELD must aggregate a particular number of routes, defined by the user, and in this scenario with only one entry point, the simulation had to include suboptimal routes for the adversary that would typically be avoided – those with a detector. While these routes were minimized, it still impacts the aggregated results, which accounts for the 92.7 success rate. When RPMs are ubiquitous in the border region, then adversary success drops to 2.0 percent, which is simply the non-detection probability of the RPM.

Random Distribution	
Holes	**Adversary Success Rate (Percent)**
40	100.0
10	100.0
9	100.0
8	100.0
7	100.0
6	100.0
5	100.0
4	99.5
3	99.2
2	97.2
1	92.8
0	1.9

Uniform Distribution	
Holes	**Adversary Success Rate (Percent)**
40	100.0
10	100.0
9	100.0
8	100.0
7	100.0
6	100.0
5	100.0
4	100.0
3	99.2
2	97.2
1	92.7
0	2.0

Clustered Distribution	
Holes	**Adversary Success Rate (Percent)**
40	100.0
10	100.0
9	100.0
8	100.0
7	100.0
6	100.0
5	100.0
4	99.5
3	98.7
2	97.1
1	92.6
0	2.0

Table 1. Symmetric network RPM sensitivities. RPMs are insensitive to the initial distribution of illegal entry points. Three network variants have nearly identical results.

In Table 2, additional tests were run with an increased non-detection probability of 0.05, to determine if this pattern was driven by the network's layout, rather than a sampling error. The same patterns emerged. Supplemental RPMs made an impact when there was only two holes in the network. This difference is primarily attributed to the increased non-detection probability. This decrease in the rate of success when there are only two holes occurs because, like above, SHIELD needs a minimum number of routes and aggregated results from suboptimal pathways. When there are no illegal entry points, the adversary's success is equal to the RPMs non-detection probability – variance in this number is again attributed to random error in Monte Carlo sampling.

From these results it is concluded that supplemental RPMs are insensitive to the initial distribution of holes in the border region; the variance in adversary success rates is attributed to random error in the sampling process.

Random Distribution	
Holes	**Adversary Success Rate (Percent)**
40	100.00
10	100.00
9	100.00
8	100.00
7	100.00
6	100.00
5	100.00
4	98.87
3	98.00
2	93.49
1	84.06
0	4.91

Uniform Distribution	
Holes	**Adversary Success Rate (Percent)**
40	100.00
10	100.00
9	100.00
8	100.00
7	100.00
6	100.00
5	100.00
4	100.00
3	98.06
2	93.46
1	84.19
0	5.06

Clustered Distribution	
Holes	**Adversary Success Rate (Percent)**
40	100.00
10	100.00
9	100.00
8	100.00
7	100.00
6	100.00
5	100.00
4	98.86
3	96.62
2	93.45
1	84.20
0	4.95

Table 2. Symmetric network with increased non-detection probabilities. RPMs with an increased non-detection probability of 0.05 are equally insensitive to the initial distribution of illegal entry points. Three network variants have nearly identical results. This pattern repeated in another run where the non-detection probability was increased to 0.20.

In all cases, the presence of RPMs only mattered when the holes in the network were below a certain threshold (Figure 10). There was no appreciable difference between a network with 35 RPMs and zero. Above that threshold, adversary failure increased slowly, with the most appreciable difference occurring when the network was completely closed off from illegal entry points. At that point it was functionally

impossible for an adversary to successful traverse the network, with a success rate based strictly on the possibility of a false-negative in the detector. This result is expected but not informative for practical purposes; it is impossible to say with certainty that every illegal entry point can be (and will continue to be) closed off to an adversary. What matters to decision-makers is the impact of RPMs on a porous border; unfortunately, RPMs demonstrate a limited utility against an informed and capable adversary.

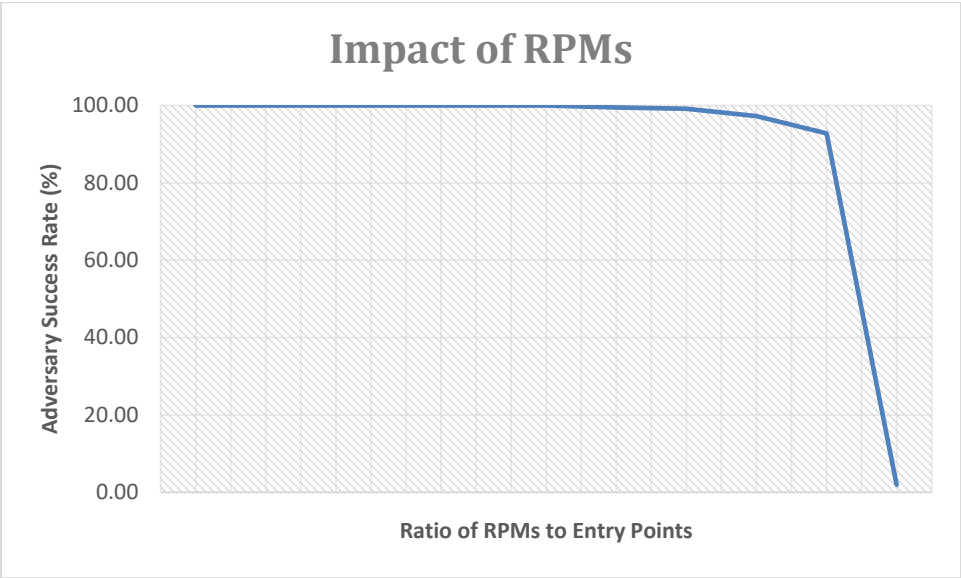

Figure 10. Impact of RPMs. Supplementing the network with additional RPMs has a negligible impact on adversary success. Additional RPMs do not have measurable impact until they are ubiquitous.

6.B. Mobile Radiation Detection Systems

A single MRDS was added to each of the network's base variants – Random, Uniform, and Clustered – with 10 holes in each network. MRDS were assigned to each of the ten positions in the provincial region of the network and tested.

	Adversary Success Rate		
	Random Distribution	**Uniform Distribution**	**Clustered Distribution**
Position 42	93.36	93.38	93.19
Position 43	93.30	93.22	93.15
Position 44	93.51	87.31	78.07
Position 45	85.41	87.70	93.11
Position 46	73.63	78.24	93.24
Position 47	83.15	86.70	93.23
Position 48	90.21	87.34	78.26
Position 49	89.90	77.33	53.29
Position 50	84.62	88.91	93.21
Position 51	64.77	74.23	93.18
Min	64.77	74.23	53.29
Max	93.51	93.38	93.24
Average	85.19	85.44	86.19

Table 3. One MRDS on the symmetric network. A single MRDS has a significant impact on the adversary's success. Here, data is aggregated from all three variants of the network, and across all principality nodes.

These initial tests proved that mobile units are highly sensitive to positioning. A single mobile unit, with an equivalent detection capability to an RPM, reduced the adversary's success by as little as 6.49 percent and by as much as 46.71 percent. The initial distribution of illegal entry points does not impact the success or failure of MRDs in the aggregate. The average success rates for adversaries on the Uniform and Random networks were within a quarter of a percent. The Clustered network has a difference of

as much as one percent (compared to the Random distribution). However, this can be attributed to a bias in SHIELD's culling procedure.

The Clustered network has the largest variance in adversary's success. This variance can be attributed to the modeling software and is not characteristic of the configuration itself. The Clustered network has holes distributed into two large clusters (Figure 11), one at the top and one at the bottom of the network. In Figure 11, dotted lines represent optimal routes favored by the adversary because they pass through a hole. There are the same number of these pathways at the top and bottom of the network. However, it so happens that SHIELDs procedure for picking and culling routes is numerical. SHIELD captures routes starting at the top of the network, and once it has reached the maximum number of routes, culls the rest. Routes at the bottom of the network tend to be culled. When positioning an MRDs at Position 51 (see Figure 11), the routes that might pass through this area tend to be culled, while routes at the top of the network, where there is no detection, are picked. The adversary's success rate of 93.18 percent for this position is inflated because of this. Overall, this increased adversary success in the Clustered network, however the increase is not real, but instead is an unintended consequence of the algorithm inside SHIELD.

Conversely, MRDS positioned at nodes 44, 48, and 49 have a minimum. These minimums exist because these MRDS are deployed close to target where a large number of routes pass through. While the adversary starts on the edge of the network where the hole clusters are, some routes cut through the middle to reach target, where they are detected by the MRDS deployed there.

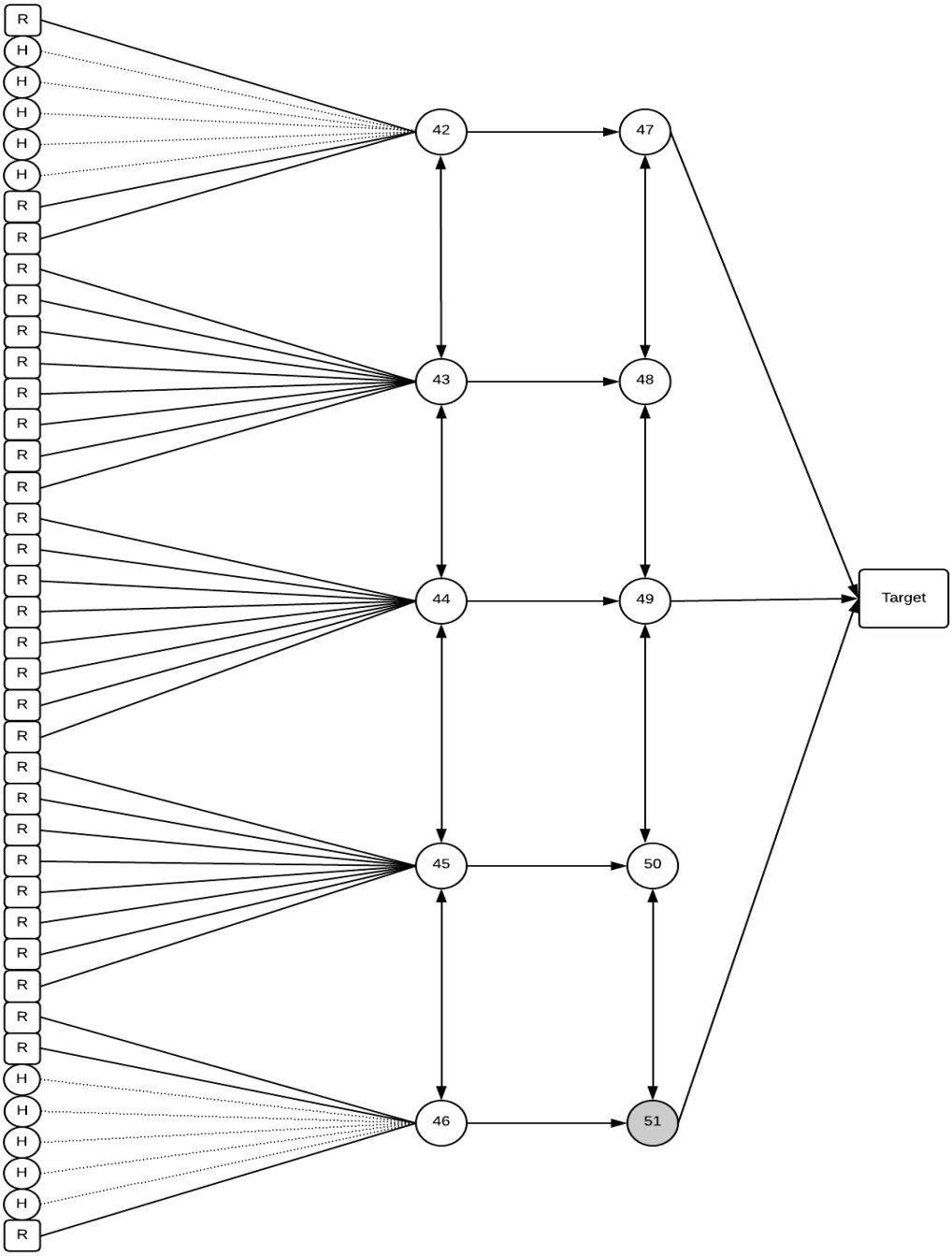

Figure 11. Clustered network pathways. The Clustered Distribution of illegal entry points in the Symmetric Network. RPMs are Squares. Holes are Circles. Dotted lines are entry-routes favored by an adversary because they pass through a hole. Position 51 at the bottom of the network is an MRD.

Additional simulations ran for a scenario with two MRDS and three MRDS on the network. MRDs were not assigned to duplicate nodes, however MRDs could be assigned to adjacent nodes resulting in an overlap in their routes and a greatly reduced non-detection probability across a single pathway (see Figure 12). Overlapping routes were treated as independent probabilities and follow the product rule for independent events. MRDS were not sampled across all potential combinations and deployment positions. Instead, a sample was taken, with deployment nodes chosen at random.

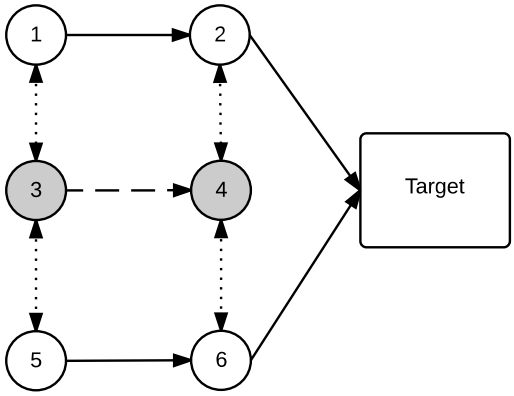

Figure 12. Overlapping MRDs routes. Nodes 3 and 4 are deployment nodes for MRDs. Pathways 3-4 (dashed line) has a non-detection probability associated with two mobile units instead of one.

Multiple MRDS suppressed the adversary's success rate even farther (Table 4 and 5). This reduction is not constant, however, which is to be expected. On average, the first MRD reduced the adversary's success by 14.39 percent (from Table 3). On average, three MRDS reduced the adversary's success by 26.38 (Table 5) when compared to a route with zero MRDS. While each additional MRDS is slightly less

effective than the previous, each MRD has a signification impact on adversary success by reducing the number of routes which can be traversed safely.

	Adversary Success Rate		
	Random	**Uniform**	**Clustered**
Position 47 51	55.31	67.80	93.16
Position 43 45	86.01	88.46	93.08
Position 50 51	62.18	72.97	93.07
Position 46 48	71.30	72.49	78.06
Position 43 49	89.46	77.90	53.24
Position 48 50	82.25	83.29	78.03
Position 42 47	82.48	86.05	93.23
Position 47 49	78.36	70.41	53.60
Position 44 51	65.64	69.08	78.14
Position 43 44	93.51	87.14	78.13
Min	55.31	67.80	53.24
Max	93.51	88.46	93.23
Average	76.65	77.56	79.17

Table 4. Two MRDs on symmetric network variants. Two MRDS on each network variant. Position combinations were chosen at random to get a sample.

	Adversary Success Rate		
	Random	**Uniform**	**Clustered**
Position 43 44 51	67.47	69.94	77.96
Position 42 48 49	87.96	74.69	44.9
Position 44 48 50	83.14	77.74	63.06
Position 48 49 50	80.45	70.51	44.97
Position 42 47 51	55.76	76.49	93.22
Position 42 45 46	70.01	79.29	93.11
Position 42 47 48	78.75	62.09	78.13
Position 44 47 51	55.48	71.59	78.18
Position 43 46 47	63.27	81.27	93.06
Position 42 45 47	75.06	67.9	93.15
Min	55.48	62.09	44.90
Max	87.96	81.27	93.22
Average	71.74	73.15	75.97

Table 5. Three MRDs on symmetric network variants. Three MRDS further suppressed adversary's success. Data is aggregated from all three variants of the network. Position combinations were chosen at random to get a sample.

Once again, the Clustered distribution has a higher adversary success rate than Random or Uniform. This was again due to SHIELD's preference for routes at the top of the network over those at the bottom (see Figure 11). With three mobile units, this preference has compounded. There is a difference of 1.41 percent between the Random and Uniform distributions, however this is still within the bounds of the model's uncertainty.

A Clustered distribution is the most conservative scenario, strictly because of this coding preference for top-of-network routes. However, this did not seem realistic. Therefore, we choose to proceed with a random distribution of illegal entry points when constructing the asymmetric network.

An initial comparison of RPMs and MRDs showed that MRDs were more effective at interdicting adversaries on the network. RPMs had a relatively negligible impact on the network until they became ubiquitous, at which point it was functionally impossible for an adversary to successfully traverse the network (Figure 10 on Page 31). On average, RPMs effected anywhere between 0 and 8.4 percent (Table 1 on Page 29) change in the adversary's success rate – as previously discussed this maximum is not real but instead is based on SHIELDs route culling algorithm which aggregates data from suboptimal routes. We therefore considered the impact of RPMs on the network without this data point. It would be more accurate to characterize the impact of RPMs as somewhere 0 and 3 percent. Whereas equivalent MRDs effected an average 14.4 percent change in the adversary's success rate.

Mobile units that enjoyed only a fraction of the efficiency of their stationary counterparts were still more effective than RPMs. A test with MRDs that were one-half, one-third, one-quarter, and one-tenth as effective as RPMs demonstrated that one MRD was still more effective than a single RPM – and often more effective than several RPMs (Table 6).

	$\varepsilon = 1$	$\varepsilon = 0.5$	$\varepsilon = 0.33$	$\varepsilon = 0.1$
Random	85.19	88.70	90.31	92.33
Uniform	85.44	88.90	90.53	92.50
Clustered	86.19	88.79	90.40	92.74

Table 6. Perturbing relative efficiency of MRDs. Three MRDS further suppressed adversary's success. Data is aggregated from all three variants of the network. Position combinations were chosen at random to get a sample.

7. ASYMMETRIC NETWORK

The asymmetric network was designed to better analyze the impact of MRDs on a network that does not possess the kind of idealized symmetry previously modeled. This network was inspired by, but does not exactly duplicate, the Texas state roadway system. Previous simulation informed the construction of this network – illegal holes were distributed randomly in the border region to analyze a conservative and realistic scenario. Entry points were reduced to 34 (instead of 40). The asymmetric network, with the initial distribution of holes and RPMs, is shown in Figure 13.

The principality region was further divided into two parts – roadways and major thoroughfares. Major thoroughfares were identified as pathways that fed into or out of major transportation hubs on the network, effectively creating choke points. MRD assignments were restricted to nodes on thoroughfares. This restriction on MRDs was designed to better simulate an intelligent and strategic deployment, exploiting the natural bottlenecks that exist in a transportation system. The network's thoroughfares are shown in Figure 14.

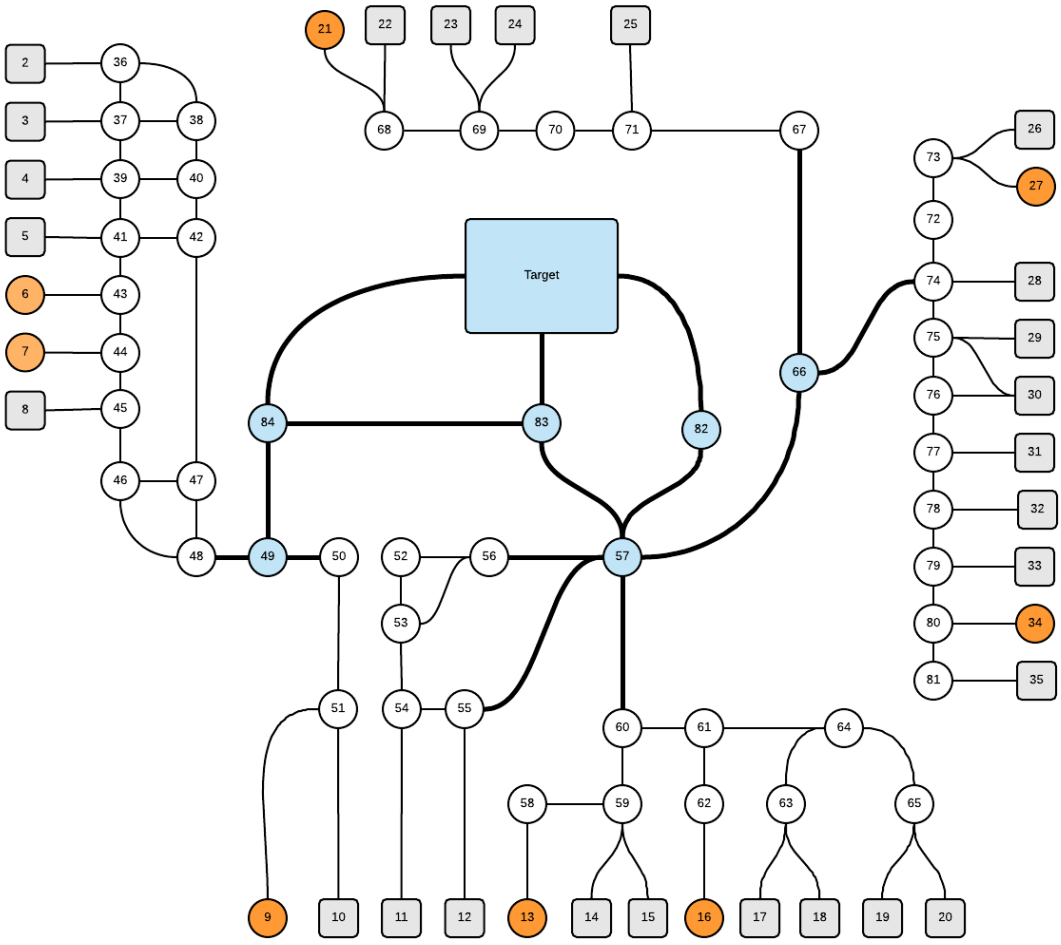

Figure 13. Complete asymmetric network. RPMs are denoted by grey boxes and illegal holes are denoted by orange circles. Through fares are denoted by bold pathways. MRD deployment nodes are marked in blue.

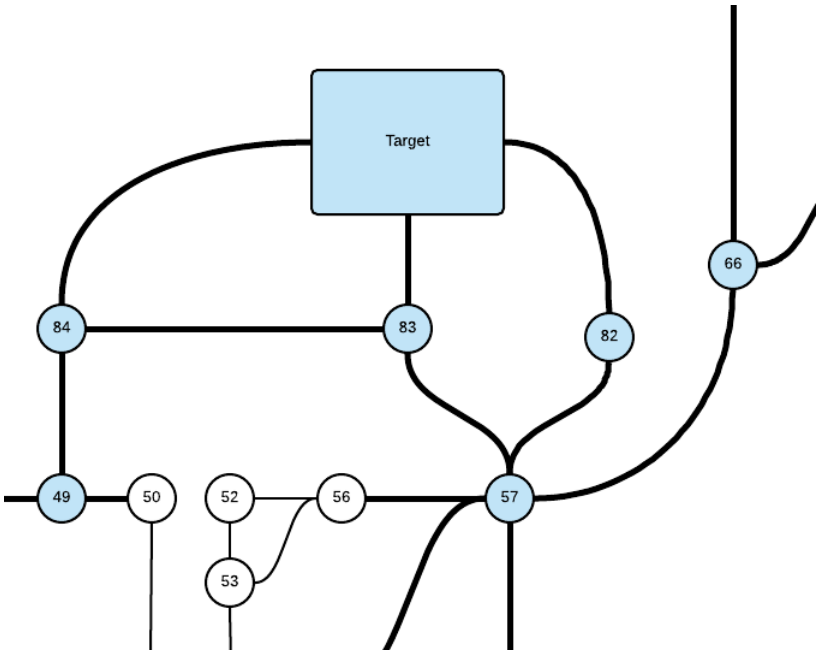

Figure 14. Major thoroughfares in the asymmetric network. Thoroughfares feed into or out of critical transportation nodes on the network. These nodes connect the border region to the larger network and to each other. MRDS deployments nodes are blue.

7.A. Radiation Portal Monitors

The network was initially tested for the impact of additional RPMs; as in the previous model RPMs were added piece-wise to the border region and tested, until all holes in the border region were closed by RPMs. Results from the asymmetric network, shown in Table 7, mirror its predecessor. RPMs had a negligible impact on adversary success until they achieved full coverage of the border region, when there are zero holes. As previously discussed this is unrealistic.

Illegal Holes	Adversary Success Rate (Percent)
8	100.00
7	100.00
6	100.00
5	100.00
4	100.00
3	99.55
2	98.74
1	97.18
0	1.92

Table 7. RPMs on the asymmetric network. RPMs have a negligible impact on the adversary's success rate until they are ubiquitous.

7.B. Mobile Radiation Detection Systems

MRDs were then tested on the asymmetric network, with a baseline of 34 entry points and 7 illegal holes (Figure 13). MRDs were initially tested with comparable efficiency to RPMs. MRDs were based out of major transportation hubs and deployed strictly to the major thoroughfares previously identified (Figure 14). Additional MRDs were added to the network and tested as well. As in the previous experiment, MRDs were never assigned to the same node but could overlap in the pathways that they covered. Once again, overlapping routes were treated as independent probabilities. Eight trials were run, one for each MRDS deployment position in the network.

Mobile units were highly effective in decreasing the adversary's success rate (Table 8). A single mobile unit of comparable efficiency to an RPM decreased the adversary's success by 20.12 percent on average. However, the variance in the

adversary's success rate tells us that MRD performance is highly sensitive to placement. Mobile units decreased adversary success by as much as 33.44 percent and as little as 5.56 percent. In a one-to-one comparison this is significantly more effective than stationary RPMs.

Position	Adversary Success Rate
Position 49	94.37
Position 57	79.17
Position 66	94.44
Position 82	85.12
Position 83	72.49
Position 84	66.56
Position 85	66.98
MIN	66.56
MAX	94.44
AVERAGE	79.88
Std. Dev	11.01

Table 8. MRDs on the asymmetric network. MRDs have a significant impact on the asymmetric network, decreasing the adversary's success rate by 20.12 percent in the aggregate. Eight trials were run to cover all eight deployment positions, with 100,000 simulations per trial.

The most effective MRDS were those positioned close to target, or that had connection to all border entry points, even if there were alternative routes. Position 84 and 83 were close to target. Both had routes to every illegal entry point. While there were also alternative routes where an adversary could have avoided the MRDS, this large footprint seems to be the key to the high impact on adversary success. Position 85, the Target, also had minimal adversary success for the same reasons. Conversely,

position 49 and position 66 had the smallest impact on the adversary. These positions covered only some of the illegal entry points into the network. Given the robust number of entry points and routes the adversary could take, these deployment positions simply did not have the kind of footprint that other deployment positions did.

Additional mobile units were then added to the model, such that every deployment position was tested in combination with a secondary deployment position. This process was repeated, to test three MRDS on a single network. Additional mobile units provided smaller non-linear returns, which is to be expected, but still had a large impact, upwards of 2.5 times the standard deviation, on the adversary's ability to successfully negotiate the network. Additional mobile units on the network have a measurable impact on the adversary's success (see Table 9). This thesis does not measure the impact of more than three mobile units on the network but does predict that as the population of MRDs grows, the adversary's success will drop off logarithmically until approaching a minimum where every thoroughfare has been blanketed with multiple MRDS.

	MRDS		
	1	**2**	**3**
MIN	66.56	44.76	34.00
MAX	94.44	79.71	64.87
AVERAGE	79.88	62.54	48.53
Std. Dev	5.28	5.91	5.56

Table 9. Additional MRDs on the asymmetric network. Additional MRDs provide diminishing returns but have a profound impact on the adversary's failure rating.

The relative efficiency of MRDS was perturbed and the simulations duplicated for a system in which MRDs possessed one-half, one-third, and one-tenth the detection capability of their RPM counterpart (See Table 10). At one-tenth relative efficiency, the MRDS still impacted the adversary's expected success rate by 2.37 percent. However, the wrapped up in this number (0.91 percent), overlaps with our results of a very effective RPM regime, which suppressed by adversary success by 2.2 percent, creating a conservative equilibrium point between these technologies. Unfortunately, it is very difficult to identify if we possess a highly effective RPM regime – one where a smuggler has very limited options for moving through illegal entry points – because the smuggler's pathways cannot be fully known[17]. We can say that this is attainable and therefore a conservative equilibrium point, is identified as one where neither technology can be said to outperform the other with certainty. An MRDS with a relative efficiency greater than one-tenth would outperform a RPM. At one-tenth it cannot be said that one

system outperforms the other. Below one-tenth, there does not appear to be a strategic benefit to MRDs.

Position	$\varepsilon = 1$	$\varepsilon = 1/2$	$\varepsilon = 1/3$	$\varepsilon = 1/10$
Position 49	94.37	91.34	93.96	98.24
Position 57	79.17	89.12	93.21	97.26
Position 66	94.44	97.00	97.93	99.38
Position 82	85.12	91.48	94.19	97.98
Position 83	72.49	85.06	89.61	97.07
Position 84	66.56	82.41	87.59	96.43
Position 85	66.98	84.13	88.99	97.02
MIN	66.56	82.41	87.59	96.43
MAX	94.44	97.00	97.93	99.38
AVERAGE	79.88	88.65	92.21	97.63
Std. Dev.	11.01	4.74	3.36	0.91

Table 10. Perturbing relative efficiency on asymmetric network. The average success rate for a single MRD of varying relative efficiencies on the asymmetrical network.

8. CONCLUSIONS

Decision makers who wish to increase our capabilities against nuclear threats must weigh the payoffs of investing further into RPMs or diversifying into MRDS. This thesis does not examine the costs associated with these choices, but it does examine the payoffs measured as a decrease in the success rate of a simulated adversary. The work here demonstrates that MRDS have a significantly higher payoff. Mobile units are discrete and while the adversary may be able to anticipate their presence, they cannot have the same confidence in their placement as a stationary (and fairly obvious) RPM. This manifests in decreased adversary success in a range of scenarios and MRDS efficiencies. The overall results of this work demonstrate that the strategic problem is insensitive to the particulars of a network. While the success rates may change the general trend is constant – MRDS are more effective.

Perturbing the efficiencies of MRDS on the network presents a target threshold for manufacturers. This work has examined MRDS with a relative efficiency of as low as 10% compared to RPMs. Although ANSI standards make the two systems practically identical, execution in a real-world scenario may drop MRD non-detection probabilities. At one-tenth relative efficiency, MRDS are comparable to RPMs. Below this value, the effectiveness of the MRDS is too small and the uncertainties too large to say with confidence that it outperforms a robust RPM program with limited pathways for an adversary. There may still be tactical advantage to an MRDS at this efficiency because of mobility, especially when complimented with actionable intelligence, but that is

beyond the scope of this work. We recommend that manufacturers aim for a system which has a non-detection capability one-tenth of an RPM or better, in a real-world application scenario.

MRDS have a higher payoff than RPMs and are worth investing in. While the costs associated with each system is not the focus of this work, it is worth acknowledging that there already exists an infrastructure for RPM deployment and use. RPMs have been well adapted into CBP and there is established protocol and norms for secondary screenings, clearing an alarm, etc. MRDS have no such infrastructure. More importantly, their mobility creates additional complication which do not exist for stationary RPMs operating at a site that is heavily controlled and monitored. What happens when a MRDS has an alarm? Who picks up the moving target? How is secondary screening handled? What is the procedure for clearing an alarm? Who has jurisdiction?

It is not the scope of this work to create or write institutional policy for MRDS. However, it is worth acknowledging that investing into MRDS means than investing into manufacturing. It also means investing into procedures and training. MRDS are an effective technology from a strategic point of view. However, to remain viable in application some care must be given to tactics, policy, and jurisdiction.

MRDS will require a means to identify targets quickly and bring them to a stop. This may mean coordination with local law enforcement or an MRDS team that has the capability to conduct a stop. Secondary screening could be conducted by a second team, local law enforcement, or the primary MRDS team. If secondary screening is conducted

by local law enforcement, that will mean making handheld detector equipment available and providing training on its use. While handheld detector software has had to become user-friendly in a post-9/11 world, this can be a large barrier if an MRDS has a large deployment area across multiple jurisdictions.

Fortunately, the FBI has already done a lot of work to create a federally lead, intelligence driven response to nuclear or radiological crisis in their annual Marble Challenge. Expanding on the work there, which is already established procedure, may be worth exploring in response to a true-positive alarm, or even during joint operations to monitor local highways. Alternatively, this could simply be handled through an interior federal investigative agency, in much the same way that other contraband smuggling cases are handled.

It may be tempting to invest in a hybrid solution, where additional RPMs are deployed state-side along major thoroughfares or choke points. While this may have value in interdicting opportunists or general deterrence, this work demonstrates that effective interdiction against an intelligent adversary requires a discrete detection system. MRDS are effective because of their ability to operate discretely. RPMs are not discrete. RPMs underperform because they can be anticipated and circumvented, not because of their network position.

Investing into additional RPMs will aid against opportunist adversaries, because the opportunist (by definition) has a limited capability to detect and avoid RPMs. Against an intelligent and capable adversary, further investment into RPMs will have a negligible impact on adversary success until they become ubiquitous. However, this is

not a practical solution for the real world where illegal entry points can be manufactured and discovered by entrepreneurial adversaries. MRDs have a measurable impact on adversary success without being omnipresent, they can be surged to protect a target when actionable intelligence is present, and they can be operated in a discrete fashion that will hinder the adversary's ability to make rational choices about successful movement.

REFERENCES

[1] White House, “National Strategy on Counterterrorism,” 2011.

[2] B. M. Jenkins, *The Likelihood of Nuclear Terror*. Santa Monica: Rand, 1985.

[3] C. C. Harmon, “Five Strategies of Terrorism,” *Small Wars Insur.*, vol. 12, no. 3, pp. 39–66, 2001.

[4] B. Hoffman, *Inside Terrorism*. New York: Columbia University Press, 2006.

[5] G. Ackerman, C. Blair, and M. Sorrells, “Radiological and Nuclear Non-State Adversaries Database (RANNSAD).” Harvard Dataverse.

[6] Department of Defense, “Proliferation, Threat and Response.” Government Printing Office, Washington, DC, 2001.

[7] White House, “National Strategy to Combat Weapons of Mass Destruction.” 2002.

[8] C. D. Ferguson and W. C. Potter, *The Four Faces of Nuclear Terrorism*. Monterey: Center for Nonproliferation Studies, 2004.

[9] D. Sanger and W. J. Broad, “U.S. Secretly Aids Pakistan in Guarding Nuclear Arms,” *The New York Times*, 18-Nov-2007.

[10] IAEA, “IAEA Incident and Traficking Database (ITDB),” 2017.

[11] DHS, “United States Customs and Border Protection’s Radiation Portal Monitors at Seaports,” 2013.

[12] Polimaster, “PM5000B Radiation Monitor Operation Manual.” 2014.

[13] IEEE, “American National Standard for Evaluation and Performance of Radiation

Detection Portal Monitors for Use in Homeland Security Accredited by the American National Standards Institute," vol. 2006, no. January. IEEE, Piscataway, 2006.

[14] K. Wood, "Deterministic Network," *Math. Comput. Model.*, vol. 17, no. 2, pp. 1–18, 1993.

[15] N. Dimitrov, D. Michalopoulos, D. Morton, M. Nehme, F. Pan, E. Popova, E. Schneider, and G. Thoreson, "Network deployment of radiation detectors with physics-based detection probability calculations," *Ann. Oper. Res.*, vol. 187, no. 1, pp. 207–228, 2011.

[16] J. Q. Cheng, M. Xie, R. Chen, and F. Roberts, "A Latent Source Model to Detect Multiple Spatial Clusters With Application in a Mobile Sensor Network for Surveillance of Nuclear Materials," *J. Am. Stat. Assoc.*, vol. 108, no. 503, pp. 902–913, 2013.

[17] C. Wang and V. M. Bier, "Optimal Defensive Allocations in the Face of Uncertain Terrorist Preferences, with an Emphasis on Transportation," *Homel. Secur. Aff.*, vol. 4, no. 4, 2012.

[18] E. Israeli and R. K. Wood, "Shortest-path network interdiction," *Networks*, vol. 40, no. 2, pp. 97–111.

[19] DHS, "CBP's Strategy to Address Illicit Cross-Border Tunnels," 2012.

[20] N. Haphuriwat, V. M. Bier, and H. H. Willis, "Deterring the Smuggling of Nuclear Weapons in Container Freight Through Detection and Retaliation," *Decis. Anal.*, vol. 8, no. 2, pp. 88–102, 2011.

[21] G. G. Thoreson and E. A. Schneider, “Efficient calculation of detection probabilities,” *Nucl. Instruments Methods Phys. Res. Sect. A Accel. Spectrometers, Detect. Assoc. Equip.*, vol. 615, no. 3, pp. 313–325, 2010.

[22] IEEE, “American National Standard Performance Criteria for Spectroscopy-Based Portal Monitors Used for Homeland Security,” *ANSI N42.38-2006*. pp. 1–45, 2007.

[23] IEEE, “American National Standard Performance Criteria for Handheld Instruments for the Detection and Identification of Radionuclides,” *ANSI N42.34-2015 (Revision of ANSI N42.34-2006)*. pp. 1–60, 2016.

[24] U.S. Department of Justice, “Police Behavior During Traffic and Street Stops, 2011,” 2013.

[25] Department of Transportation, “Average Annual Miles per Driver per Age Group,” 2015.

APPENDIX A

Sample Input Deck

```
C---------------------------------------
C
C   SHIELD program version 26.0.0.0
C   Developed By Nuclear Security Science & Policy Institute (NSSPI)
C   Saved Input file
C   Saved Date and Time: 5/24/2012 11:43:45 PM
C
C---------------------------------------
C
C   run_number, HEU_quality, Container_type
       100000;        1.5;            3;
C
C (print control) Title, Summary, Input, Bin, Routes, Links, Nodes
                  1;      1;    1;   1;     1;    1;    1;
C
C Behavior mode (1 for Step by Step, 0 for intelligent), routes selection num, seed value method, seed value
                                        0;              5;              0;
C
C Total dataset number
10;
C Layer Num, Min nPD lim, Max nPD lim;
1;                    0.1;   0.9;
2;                    0.1;   0.9;
3;                    0.1;   0.9;
4;                    0.1;   0.9;
5;                    0.1;   0.9;
6;                    0.1;   0.9;
7;                    0.1;   0.9;
8;                    0.1;   0.9;
9;                    0.1;   0.9;
10;                   0.1;   0.9;
C
C Node number, initial node, end node
         8;          1;       8;
C
C - Node   1, node number, perceived nPD, actual nPD, forward paths number, time, redirect_prob,group, description, location,    latitude,   longitude,
```

N; 1; 0.4; 0.6; 1; 2; 0.2; 1; port; Houston; 29.7631; -95.3631;
C - Pathway from node 1, initial node, end node, group, distance, time, perceived nPD, actual nPD, description
P; 1; 2; 2; 100.00; 2; 0.5; 0.7; 1;
C
C - Node 2, node number, perceived nPD, actual nPD, forward paths number, time, redirect_prob,group, description, location, latitude, longitude,
N; 2; 0.3; 0.6; 3; 3; 0.5; 2;City airport; New York; 40.7142; -74.0064;
C - Pathway from node 2, initial node, end node, group, distance, time, perceived nPD, actual nPD, description
P; 2; 3; 3; 200.00; 4; 0.6; 0.45; h;
P; 2; 4; 3; 200.00; 4; 0.3; 0.5; h;
P; 2; 5; 3; 200.00; 4; 0.5; 0.5; h;
C
C - Node 3, node number, perceived nPD, actual nPD, forward paths number, time, redirect_prob,group, description, location, latitude, longitude,
N; 3; 0.35; 0.5; 1; 3; 0.5; 3; train;Los Angeles; 34.0522; -118.2428;
C - Pathway from node 3, initial node, end node, group, distance, time, perceived nPD, actual nPD, description
P; 3; 6; 4; 100.00; 2; 0.4;0.55; a;
C
C - Node 4, node number, perceived nPD, actual nPD, forward paths number, time, redirect_prob,group, description, location, latitude, longitude,
N; 4; 0.7; 0.3; 1; 3; 1; 3; truck; Beijing; 39.9100; 116.4000;
C - Pathway from node 4, initial node, end node, group, distance, time, perceived nPD, actual nPD, description
P; 4; 7; 4; 100.00; 2; 0.6; 0.5; a;
C
C - Node 5, node number, perceived nPD, actual nPD, forward paths number, time, redirect_prob,group, description, location, latitude, longitude,
N; 5; 0.6; 0.4; 1; 3; 0; 4; ship; Tokyo; 35.6833; 139.7667;
C - Pathway from node 5, initial node, end node, group, distance, time, perceived nPD, actual nPD, description
P; 5; 8; 5; 100.00; 2; 0.65; 0.5; a;
C
C - Node 6, node number, perceived nPD, actual nPD, forward paths number, time, redirect_prob,group, description, location, latitude, longitude,
N; 6; 0.8;0.6; 1; 3; 1; 5; airport; Chicago; 41.8500; -87.6500;

C - Pathway from node 6, initial node, end node, group, distance, time, perceived nPD, actual nPD, description
P; 6; 8; 6; 100.00; 2; 0.4; 0.5; a;
C
C - Node 7, node number, perceived nPD, actual nPD, forward paths number, time, redirect_prob,group, description, location, latitude, longitude,
N; 7; 0.8; 0.6; 1; 3; 0.3; 5; airport; Paris; 48.8742; 2.3470;
C - Pathway from node 7, initial node, end node, group, distance, time, perceived nPD, actual nPD, description
P; 7; 8; 6; 100.00; 2; 0.5; 0.5; a;
C
C - Node 8, node number, perceived nPD, actual nPD, forward paths number, time, redirect_prob,group, description, location, latitude, longitude,
N; 8; 0.5; 0.6; 0; 3; 0.2; 6; airport; Roma; 41.9000; 12.5000;
C - Pathway from node 8, initial node, end node, group, distance, time, perceived nPD, actual nPD, description
C
C----------
C
C End of Input file
C
C----------